100 XP

Introduction

1 minute

As more business data is being accessed from locations outside of the traditional corporate network, security and compliance have become overriding concerns. Organizations need to understand how they can best protect their data, regardless of where it's accessed from, and whether it sits on their corporate network or in the cloud. In addition, organizations need to ensure they're compliant with industry and regulatory requirements to ensure the protection and privacy of data.

This module introduces some important security and compliance concepts. You'll learn about the shared responsibility model, defense in depth, and Zero Trust model. You'll be introduced to the concepts of encryption and hashing as ways to protect data. Lastly, you'll learn about concepts that relate to compliance.

After completing this module, you'll be able to:

- **Describe the shared responsibility and the defense in-depth security models.**
- **Describe the Zero-Trust model.**
- **Describe the concepts of encryption and hashing.**
- **Describe some basic compliance concepts.**

Next unit: Describe the shared responsibility model

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe the shared responsibility model

3 minutes

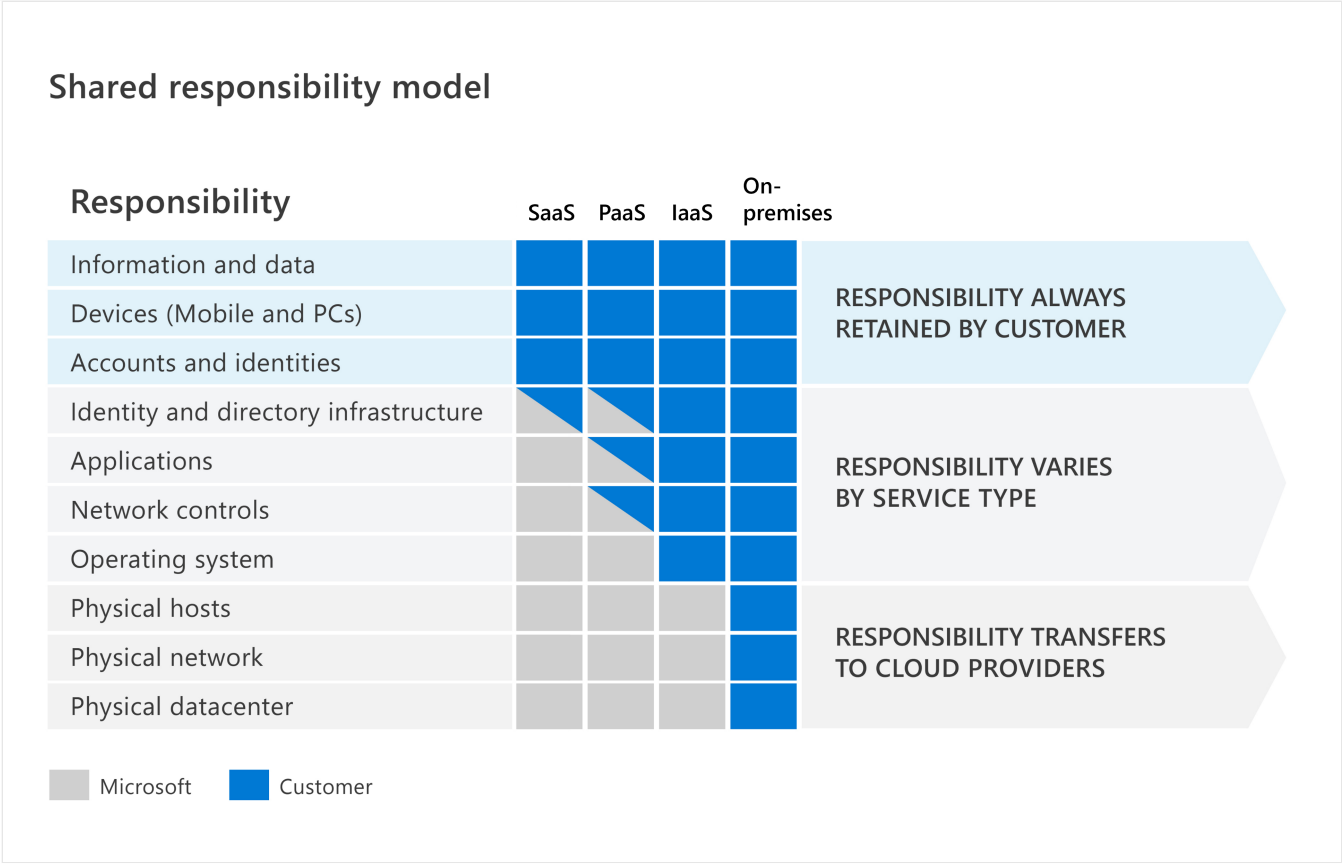
In organizations running only on-premises hardware and software, the organization is 100 percent responsible for implementing security and compliance. With cloud-based services, that responsibility is shared between the customer and the cloud provider.

The *shared responsibility model* identifies which security tasks are handled by the cloud provider, and which security tasks are handled by you, the customer. The responsibilities vary depending on where the workload is hosted:

- **Software as a Service (SaaS)**
- **Platform as a Service (PaaS)**
- **Infrastructure as a Service (IaaS)**
- **On-premises datacenter**

The shared responsibility model makes responsibilities clear. When organizations move to the cloud, some responsibilities transfer to the cloud provider and some to the customer organization.

The following diagram illustrates the areas of responsibility between the customer and the cloud provider, according to where data is held.



- **On-premises datacenters. In an on-premises datacenter, you have responsibility for everything from physical security to encrypting sensitive data.**
- **Infrastructure as a Service (IaaS). Of all cloud services, IaaS requires the most management by the cloud customer. With IaaS, you're using the cloud provider's computing infrastructure. The cloud customer isn't responsible for the physical components, such as computers, the network, or the physical security of the datacenter. However, the cloud customer still has responsibility for software components running on that computing infrastructure such as operating systems, network controls, applications, and protecting data.**
- **Platform as a Service (PaaS). PaaS provides an environment for building, testing, and deploying software applications. The goal of PaaS is to help you create an application quickly without managing the underlying infrastructure. With PaaS, the cloud provider manages the hardware and operating systems, and the customer is responsible for applications and data.**
- **Software as a Service (SaaS). SaaS is hosted and managed by the cloud provider, for the customer. It's usually licensed through a monthly or annual subscription. Microsoft 365, Skype, and Dynamics CRM Online are all examples of SaaS software. SaaS requires the least amount of management by the cloud customer. The cloud provider is responsible for managing everything except data, devices, accounts, and identities.**

For all cloud deployment types you, the cloud customer, own your data and identities. You're responsible for protecting the security of your data and identities, and on-premises resources including mobile devices, PCs, printers, and more.

In summary, responsibilities always retained by the customer organization include:

- **Information and data**
- **Devices (mobile and PCs)**
- **Accounts and identities**

The benefit of the shared responsibility model is that organizations are clear about their responsibilities, and those of the cloud provider.

Next unit: Describe defense in depth

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

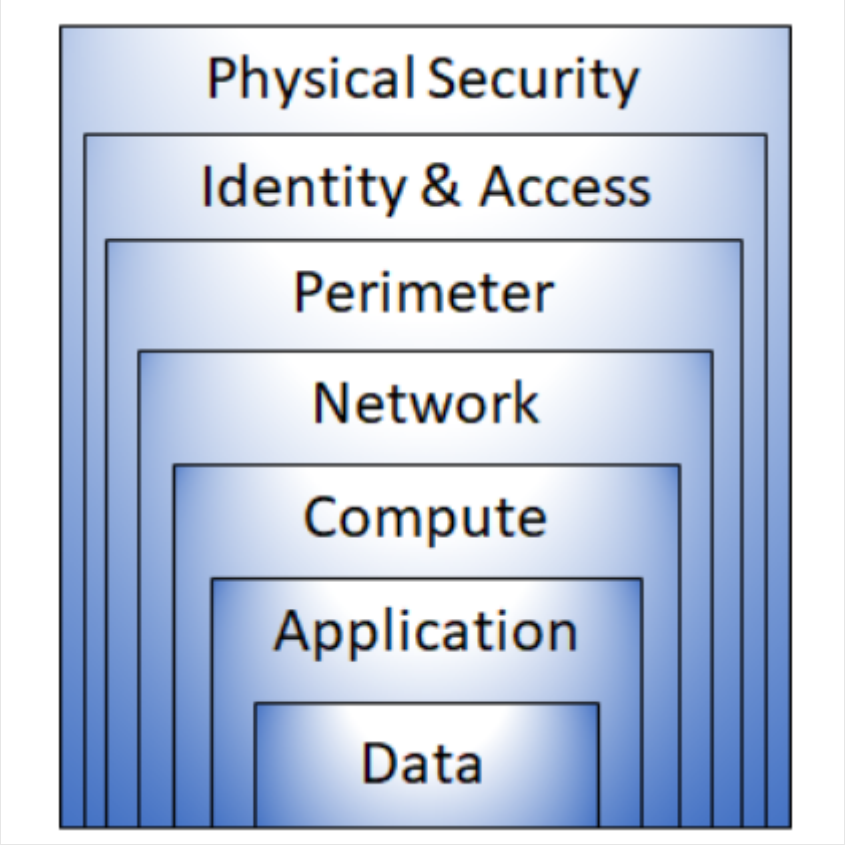
Describe defense in depth

4 minutes

Defense in depth uses a layered approach to security, rather than relying on a single perimeter. A defense in-depth strategy uses a series of mechanisms to slow the advance of an attack. Each layer provides protection so that, if one layer is breached, a subsequent layer will prevent an attacker getting unauthorized access to data.

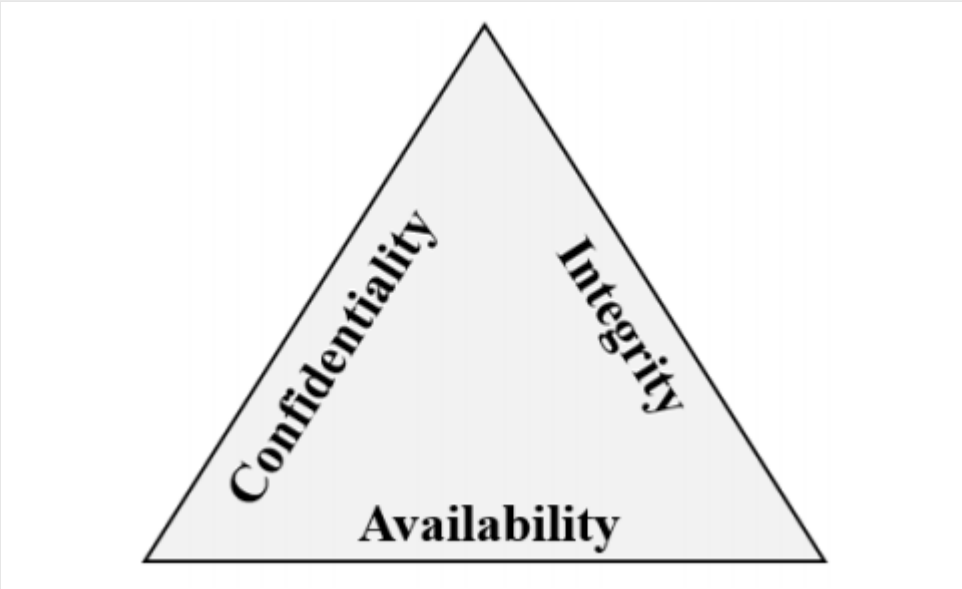
Example layers of security might include:

- **Physical security such as limiting access to a datacenter to only authorized personnel.**
- **Identity and access security controls, such as multifactor authentication or condition-based access, to control access to infrastructure and change control.**
- **Perimeter security of your corporate network includes distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.**
- **Network security, such as network segmentation and network access controls, to limit communication between resources.**
- **Compute layer security such as securing access to virtual machines either on-premises or in the cloud by closing certain ports.**
- **Application layer security to ensure applications are secure and free of security vulnerabilities.**
- **Data layer security including controls to manage access to business and customer data and encryption to protect data.**



Confidentiality, Integrity, Availability (CIA)

As described above, a defense in-depth strategy uses a series of mechanisms to slow the advance of an attack. All the different mechanisms (technologies, processes, and training) are elements of a cybersecurity strategy, whose goals include ensuring confidentiality, integrity, and availability; often referred to as CIA.



- **Confidentiality refers to the need to keep confidential sensitive data such as customer information, passwords, or financial data. You can encrypt data to keep it confidential, but then you also need to keep the encryption keys confidential.**

Confidentiality is the most visible part of security; we can clearly see need for sensitive data, keys, passwords, and other secrets to be kept confidential.

- **Integrity refers to keeping data or messages correct. When you send an email message, you want to be sure that the message received is the same as the message you sent. When you store data in a database, you want to be sure that the data you retrieve is the same as the data you stored. Encrypting data keeps it confidential, but you must then be able to decrypt it so that it's the same as before it was encrypted. Integrity is about having confidence that data hasn't been tampered with or altered.**
- **Availability refers to making data available to those who need it, when they need it. It's important to the organization to keep customer data secure, but at the same time it must also be available to employees who deal with customers. While it might be more secure to store the data in an encrypted format, employees need access to decrypted data.**

While the goals of a cybersecurity strategy are to preserve the confidentiality, integrity, and availability of systems, networks, applications, and data; it's the goal of cybercriminals to disrupt these goals. Microsoft's portfolio includes the solutions and technologies to enable organizations to deliver on the goals of the CIA triad.

Next unit: Describe the Zero Trust model

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe the Zero Trust model

5 minutes

Zero Trust assumes everything is on an open and untrusted network, even resources behind the firewalls of the corporate network. The Zero Trust model operates on the principle of "trust no one, verify everything."

Attackers' ability to bypass conventional access controls is ending any illusion that traditional security strategies are sufficient. By no longer trusting the integrity of the corporate network, security is strengthened.

In practice, this means that we no longer assume that a password is sufficient to validate a user but add multi-factor authentication to provide additional checks. Instead of granting access to all devices on the corporate network, users are allowed access only to the specific applications or data that they need.

This video introduces the Zero Trust methodology:

Zero Trust guiding principles

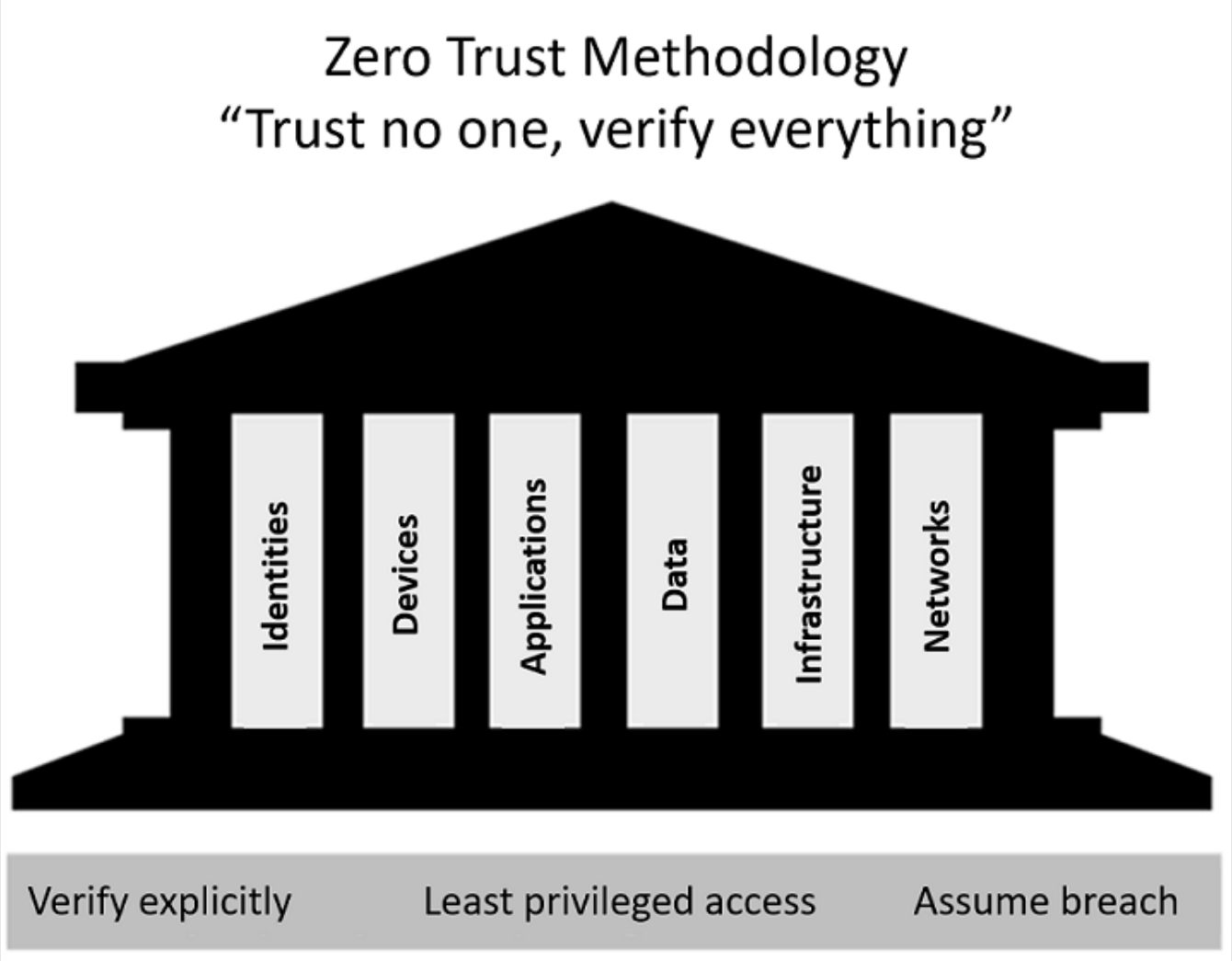
The Zero Trust model has three principles which guide and underpin how security is implemented. These are: verify explicitly, least privilege access, and assume breach.

- **Verify explicitly. Always authenticate and authorize based on the available data points, including user identity, location, device, service or workload, data classification, and anomalies.**
- **Least privileged access. Limit user access with just-in-time and just-enough access (JIT/JEA), risk-based adaptive policies, and data protection to protect both data and productivity.**
- **Assume breach. Segment access by network, user, devices, and application. Use encryption to protect data, and use analytics to get visibility, detect threats, and improve your security.**

Six foundational pillars

In the Zero Trust model, all elements work together to provide end-to-end security. These six elements are the foundational pillars of the Zero Trust model:

- **Identities may be users, services, or devices. When an identity attempts to access a resource, it must be verified with strong authentication, and follow least privilege access principles.**
- **Devices create a large attack surface as data flows from devices to on-premises workloads and the cloud. Monitoring devices for health and compliance is an important aspect of security.**
- **Applications are the way that data is consumed. This includes discovering all applications being used, sometimes called Shadow IT because not all applications are managed centrally. This pillar also includes managing permissions and access.**
- **Data should be classified, labeled, and encrypted based on its attributes. Security efforts are ultimately about protecting data, and ensuring it remains safe when it leaves devices, applications, infrastructure, and networks that the organization controls.**
- **Infrastructure, whether on-premises or cloud based, represents a threat vector. To improve security, you assess for version, configuration, and JIT access, and use telemetry to detect attacks and anomalies. This allows you to automatically block or flag risky behavior and take protective actions.**
- **Networks should be segmented, including deeper in-network micro segmentation. Also, real-time threat protection, end-to-end encryption, monitoring, and analytics should be employed.**



A security strategy that employs the three principles of the Zero Trust model across the six foundational pillars helps companies deliver and enforce security across their organization.

Next unit: Describe encryption and hashing

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

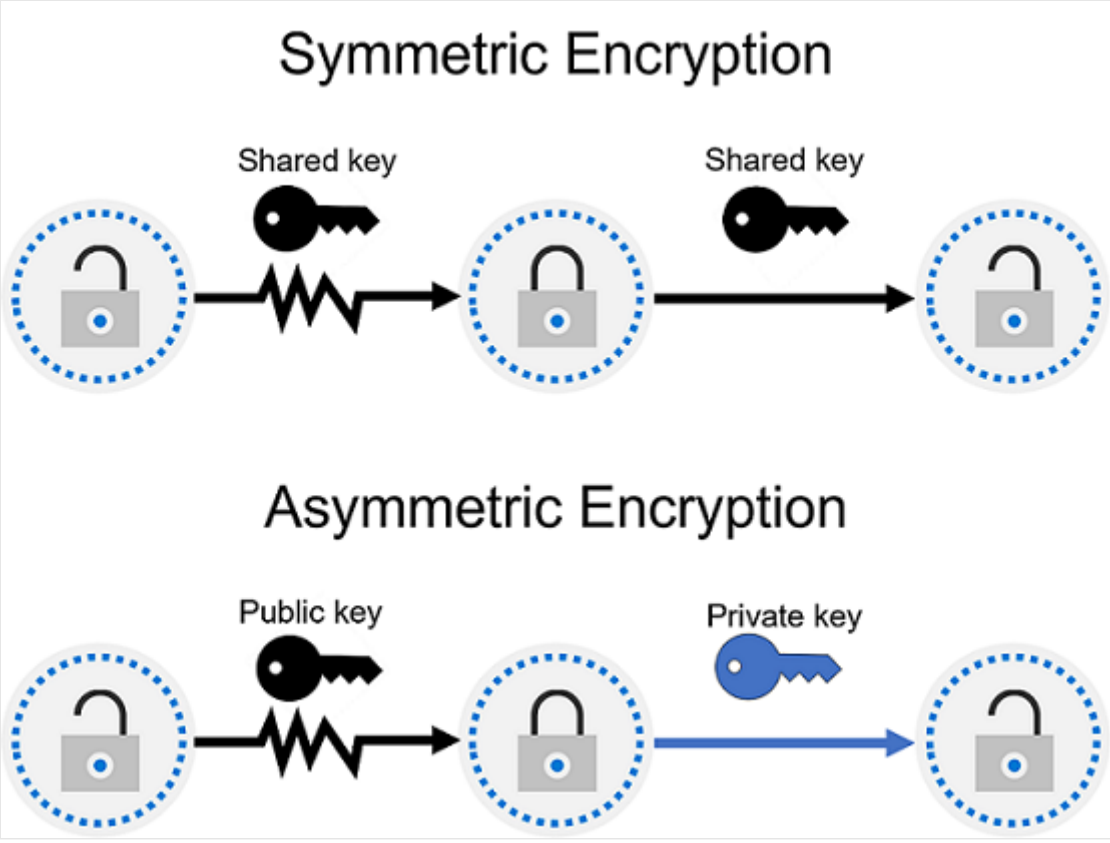
100 XP

Describe encryption and hashing

4 minutes

One way to mitigate against common cybersecurity threats is to encrypt sensitive or valuable data. Encryption is the process of making data unreadable and unusable to unauthorized viewers. To use or read encrypted data, it must be decrypted, which requires the use of a secret key.

There are two top-level types of encryption: symmetric and asymmetric. Symmetric encryption uses the same key to encrypt and decrypt the data. Asymmetric encryption uses a public key and private key pair. Either key can encrypt data, but the key used to encrypt can't be used to decrypt encrypted data. To decrypt, you need a paired key. For example, if the public key is used to encrypt, then only the corresponding private key can be used to decrypt. Asymmetric encryption is used for things such accessing sites on the internet using the HTTPS protocol and electronic data signing solutions. Encryption may protect data at rest, or in transit. For additional information on the concepts of cryptography, refer to Describe concepts of cryptography



Encryption for data at rest

Data at rest is the data that's stored on a physical device, such as a server. It may be stored in a database or a storage account but, regardless of where it's stored, encryption of data at rest ensures the data is unreadable without the keys and secrets needed to decrypt it.

If an attacker obtained a hard drive with encrypted data and didn't have access to the encryption keys, they would be unable to read the data.

Encryption for data in transit

Data in transit is the data moving from one location to another, such as across the internet or through a private network. Secure transfer can be handled by several different layers. It could be done by encrypting the data at the application layer before sending it over a network. HTTPS is an example of encryption in transit.

Encrypting data in transit protects it from outside observers and provides a mechanism to transmit data while limiting the risk of exposure.

Encryption for data in use

A common use case for encryption of data in use involves securing data in nonpersistent storage, such as RAM or CPU caches. This can be achieved through technologies that create an enclave (think of this as a secured lockbox) that protects the data and keeps data encrypted while the CPU processes the data.

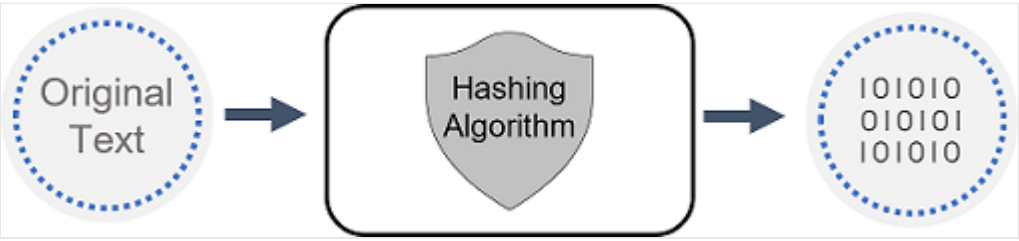
Hashing

Hashing uses an algorithm to convert text to a *unique* fixed-length value called a hash. Each time the same text is hashed using the same algorithm, the same hash value is produced. That hash can then be used as a unique identifier of its associated data.

Hashing is different to encryption in that it doesn't use keys, and the hashed value isn't subsequently decrypted back to the original.

Hashing is often used to store passwords. When a user enters their password, the same algorithm that created the stored hash creates a hash of the entered password. This is compared to the stored hashed version of the password. If they match, the user has entered their password correctly. This is more secure than storing plain text passwords, but hashing algorithms are also known to hackers. Because hash functions are deterministic (the same input produces the same output), hackers can use brute-force dictionary attacks by hashing the passwords. For every matched hash, they know the

actual password. To mitigate this risk, passwords are often "salted". This refers to adding a fixed-length random value to the input of hash functions to create unique hashes for same input.



Next unit: Describe governance, risk, and compliance (GRC) concepts

Continue >

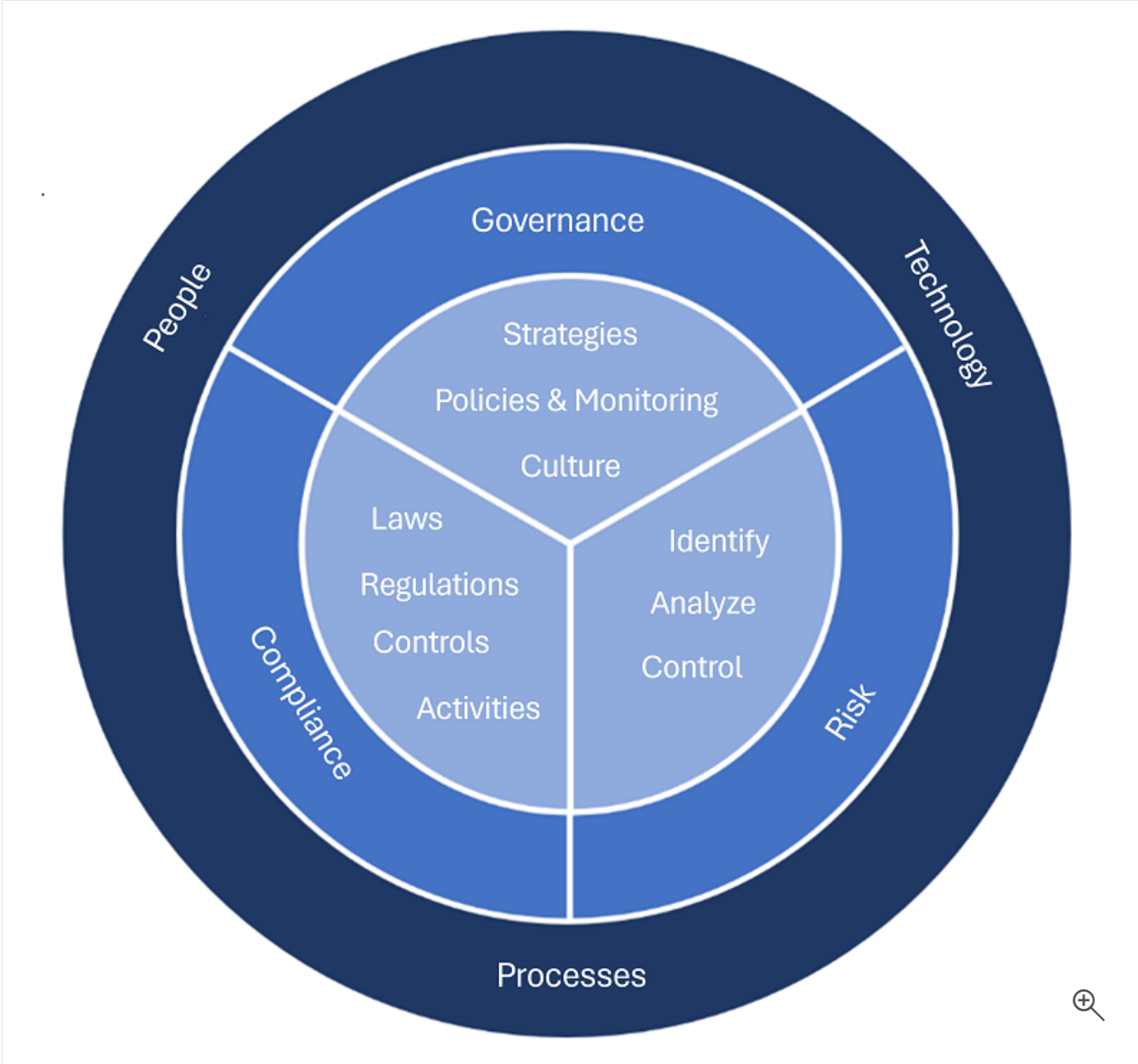
How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe governance, risk, and compliance (GRC) concepts

2 minutes

Organizations face increasing complexity and change in regulatory environments, calling for a more structured approach for managing Governance, Risk, and Compliance (GRC).



As organizations establish GRC competency they can establish a framework that includes implementing specific policies, operational processes. A structured approach for managing GRC helps organizations reduce risk and improve compliance effectiveness.

An important prerequisite to establishing GRC competency is understanding the key terms.

Governance

Governance is the system of rules, practices, and processes an organization uses to direct and control its activities. Many governance activities arise from external standards, obligations and expectations. For example, organizations establish rules and process that define the who, what, where, and when users and applications can access corporate resources and who has administrative privileges and for how long.

Risk

Risk management is the process of identifying, assessing, and responding to threats or events that can impact company or customer objectives. Organizations face risk from both external and internal sources. External risks can come from political and economic forces weather related events, pandemics, and security breaches to name just a few sources. Internal risks are risks that come from within the organization itself. Examples include leaks of sensitive data, intellectual property theft, fraud, and insider trading.

Compliance

Compliance refers to the country/region, state or federal laws or even multi-national regulations that an organization must follow. These regulations define what types of data must be protected, what processes are required under the legislation, and what penalties are issued to organizations that fail to comply.

It's important to note that compliance is not the same as security. But, security should be considered when building a compliance plan as effective security is frequently a compliance requirement. Compliance requires only that the legally mandated minimum standards are met whereas data security covers all the processes, procedures and technologies that define how you look after sensitive data and guard against breaches.

Some compliance-related concepts include:

- **Data residency - When it comes to compliance, data residency regulations govern the physical locations where data can be stored and how and when it can be transferred, processed, or accessed internationally. These regulations can differ significantly depending on jurisdiction.**
- **Data sovereignty - Another important consideration is data sovereignty, the concept that data, particularly personal data, is subject to the laws and regulations**

of the country/region in which it's physically collected, held, or processed. This can add a layer of complexity when it comes to compliance because the same piece of data can be collected in one location, stored in another, and processed in still another; making it subject to laws from different countries/regions.

- **Data privacy - Providing notice and being transparent about the collection, processing, use, and sharing of personal data are fundamental principles of privacy laws and regulations. Personal data means any information relating to an identified or identifiable natural person. Privacy laws encompass any data that is directly linked or indirectly linkable back to a person. Organizations are subject to, and must operate consistent with, a multitude of laws, regulations, codes of conduct, industry-specific standards, and compliance standards governing data privacy.**

Next unit: Knowledge check

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Summary and resources

1 minute

In this module you were introduced to some important security and compliance concepts. You learned about the shared responsibility model and how the workload responsibilities vary depending on where the workload is hosted. You learned how a defense in-depth strategy uses a series of mechanisms to slow the advance of an attack. You learned about the guiding principles of Zero Trust and how the six foundational pillars work together to enforce organization security policies. Lastly, you were introduced to the concepts of encryption and hashing as ways to secure your data and some basic concepts related to data compliance.

Now that you've completed this module, you should be able to:

- **Describe the shared responsibility and the defense in-depth security models.**
- **Describe the Zero-Trust model.**
- **Describe the concepts of encryption and hashing.**
- **Describe some basic compliance concepts.**

Learn more

To learn more about the topics discussed in this module, see:

- **Zero Trust Resource Center**
- **Shared responsibility in the cloud**
- **Azure defense in depth**
- **Enabling Data Residency and Data Protection in Microsoft Azure Regions**
- **Describe concepts of cryptography**

Module complete:

Review your Learning Path history

Explore other paths

100 XP

Introduction

1 minute

Everyone, and every device, has an identity that can be used to access resources. Identity is the way in which people and things are identified on your corporate network, and in the cloud. Being certain about who or what is accessing your organization's data and other resources is a fundamental part of securing your environment.

In this module, you'll learn about the key concepts of authentication and authorization and why identity is important in securing corporate resources. You'll also learn about some identity related services.

After completing this module, you'll be able to:

- **Understand the difference between authentication and authorization.**
- **Describe the concept of identity as a security perimeter.**
- **Describe identity-related services.**

Next unit: Define authentication and authorization

Continue

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Define authentication and authorization

2 minutes

Authentication

Authentication is the process of proving that a person is who they say they are. When someone purchases an item with a credit card, they may be required to show an additional form of identification. This proves that they are the person whose name appears on the card. In this example, the user may show a driver's license that serves as a form of authentication and proves their ID.

When you want to access a computer or device, you'll encounter a similar type of authentication. You may get asked to enter a username and password. The username states who you are, but by itself isn't enough to grant you access. When combined with the password, which only that user should know, it allows access to your systems. The username and password, together, are a form of authentication. Authentication is sometimes shortened to AuthN.

Authorization

Once you authenticate a user, you'll need to decide where they can go, and what they're allowed to see and touch. This process is called authorization.

Suppose you want to spend the night in a hotel. The first thing you'll do is go to reception to start the "authentication process". After the receptionist has verified who you are, you're given a keycard and can go to your room. Think of the keycard as the authorization process. The keycard will only let you open the doors and elevators you're permitted to access, such as for your hotel room.

In cybersecurity terms, authorization determines the level of access or the permissions an authenticated person has to your data and resources. Authorization is sometimes shortened to AuthZ.

Next unit: Define identity as the primary security perimeter

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Define identity as the primary security perimeter

3 minutes

Digital collaboration has changed. Your employees and partners now need to collaborate and access organizational resources from anywhere, on any device, and without affecting their productivity. There has also been an acceleration in the number of people working from home.

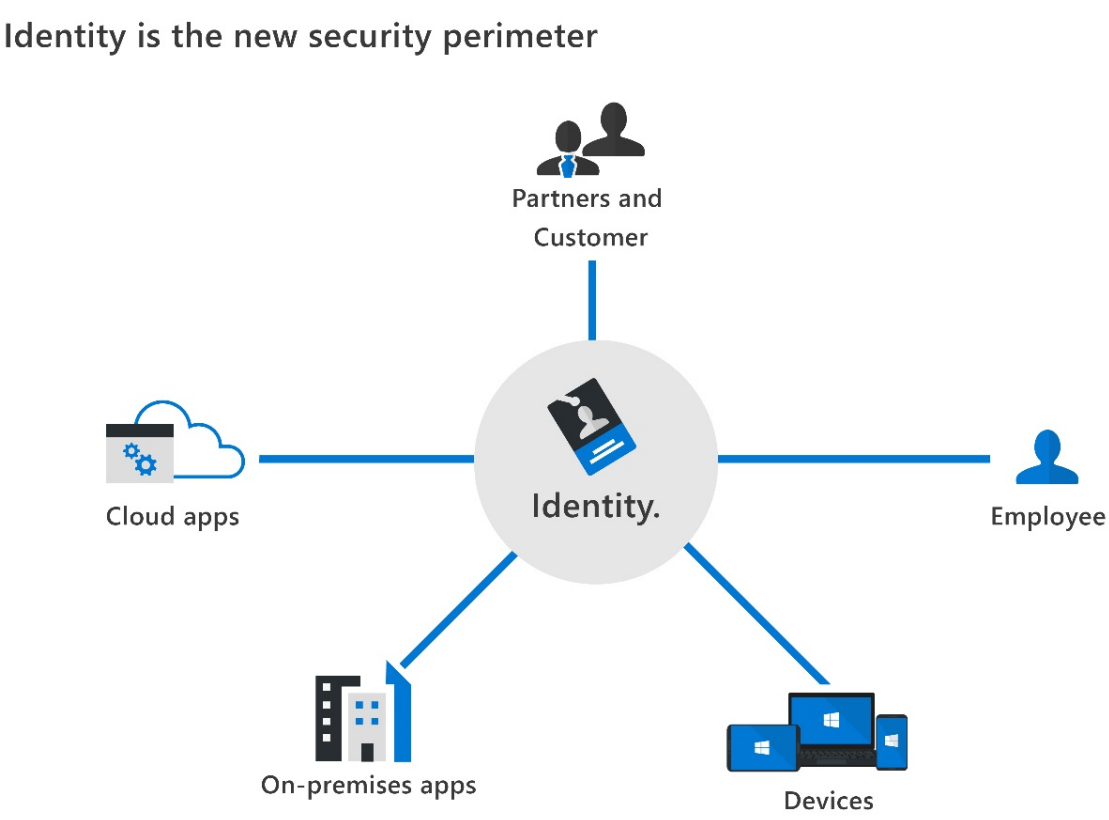
Enterprise security needs to adapt to this new reality. The security perimeter can no longer be viewed as the on-premises network. It now extends to:

- **SaaS applications for business-critical workloads that might be hosted outside the corporate network.**
- **The personal devices that employees are using to access corporate resources (BYOD, or bring your own device) while working from home.**
- **The unmanaged devices used by partners or customers when interacting with corporate data or collaborating with employees**
- **Internet of things, referred to as IoT devices, installed throughout your corporate network and inside customer locations.**

The traditional perimeter-based security model is no longer enough. Identity has become the new security perimeter that enables organizations to secure their assets.

But what do we mean by an identity? An identity is the set of things that define or characterize someone or something. For example, a person's identity includes the information they use to authenticate themselves, such, as their username and password and their level of authorization.

An identity may be associated with a user, an application, a device, or something else.



Four pillars of an identity infrastructure

Identity is a concept that spans an entire environment, so organizations need to think about it broadly. There's a collection of processes, technologies, and policies for managing digital identities and controlling how they're used to access resources. These can be organized into four fundamental pillars that organizations should consider when creating an identity infrastructure.

- **Administration. Administration is about the creation and management/governance of identities for users, devices, and services. As an administrator, you manage how and under what circumstances the characteristics of identities can change (be created, updated, deleted).**
- **Authentication. The authentication pillar tells the story of how much an IT system needs to know about an identity to have sufficient proof that they really are who they say they are. It involves the act of challenging a party for legitimate credentials.**
- **Authorization. The authorization pillar is about processing the incoming identity data to determine the level of access an authenticated person or service has within the application or service that it wants to access.**
- **Auditing. The auditing pillar is about tracking who does what, when, where, and how. Auditing includes having in-depth reporting, alerts, and governance of identities.**

Addressing each of these four pillars is key to a comprehensive and robust identity and access control solution.

Next unit: Describe the role of the identity provider

Continue >

100 XP

Describe the role of the identity provider

7 minutes

Modern authentication **is an umbrella term for authentication and authorization methods between a client, such as your laptop or phone, and a server, like a website or application. At the center of modern authentication is the role of the *identity provider*. An identity provider creates, maintains, and manages identity information while offering authentication, authorization, and auditing services.**

With modern authentication, all services, including all authentication services, are supplied by a central identity provider. Information that's used to authenticate the user with the server is stored and managed centrally by the identity provider.

With a central identity provider, organizations can establish authentication and authorization policies, monitor user behavior, identify suspicious activities, and reduce malicious attacks.

Watch this video for more information about modern authentication and how it works with a central identity provider.

As you see in the video, thanks to modern authentication, the client communicates with the identity provider by giving an identity that can be authenticated. When the identity (which can be a user or an application) has been verified, the identity provider issues a *security token* that the client sends to the server.

The server validates the security token through its *trust relationship* with the identity provider. By using the security token and the information that's contained within it, the user or application accesses the required resources on the server. In this scenario, the token and the information it contains is stored and managed by the identity provider. The centralized identity provider is supplying the authentication service.

Microsoft Azure Active Directory is an example of a cloud-based identity provider. Other examples include Twitter, Google, Amazon, LinkedIn, and GitHub.

Single sign-on

Another fundamental capability of an identity provider and "modern authentication" is the support for single sign-on (SSO). With SSO, the user logs in once and that credential

is used to access multiple applications or resources. When you set up SSO between multiple identity providers, it's called federation.

Next unit: Describe the concept of directory services and Active Directory

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe the concept of directory services and Active Directory

2 minutes

In the context of a computer network, a directory is a hierarchical structure that stores information about objects on the network. A directory service stores directory data and makes it available to network users, administrators, services, and applications.

Active Directory (AD) is a set of directory services developed by Microsoft as part of Windows 2000 for on-premises domain-based networks. The best-known service of this kind is Active Directory Domain Services (AD DS). It stores information about members of the domain, including devices and users, verifies their credentials, and defines their access rights. A server running AD DS is a domain controller (DC).

AD DS is a central component in organizations with on-premises IT infrastructure. AD DS gives organizations the ability to manage multiple on-premises infrastructure components and systems using a single identity per user. AD DS doesn't, however, natively support mobile devices, SaaS applications, or line of business apps that require *modern authentication* methods.

The growth of cloud services, SaaS applications, and personal devices being used at work, has resulted in the need for modern authentication, and an evolution of Active Directory-based identity solutions.

Microsoft Entra ID, previously referred to as Azure Active Directory (Azure AD) and part of the Microsoft Entra family of multicloud identity and access solutions, is an example of the evolution of identity and access management solutions. It provides organizations with an Identity as a Service (IDaaS) solution for all their apps across cloud and on-premises.

To learn more about the differences between Active Directory concepts and Microsoft Entra ID, refer to the Learn More section of the Summary and resources unit that links to documentation.

Next unit: Describe the concept of federation

Continue >

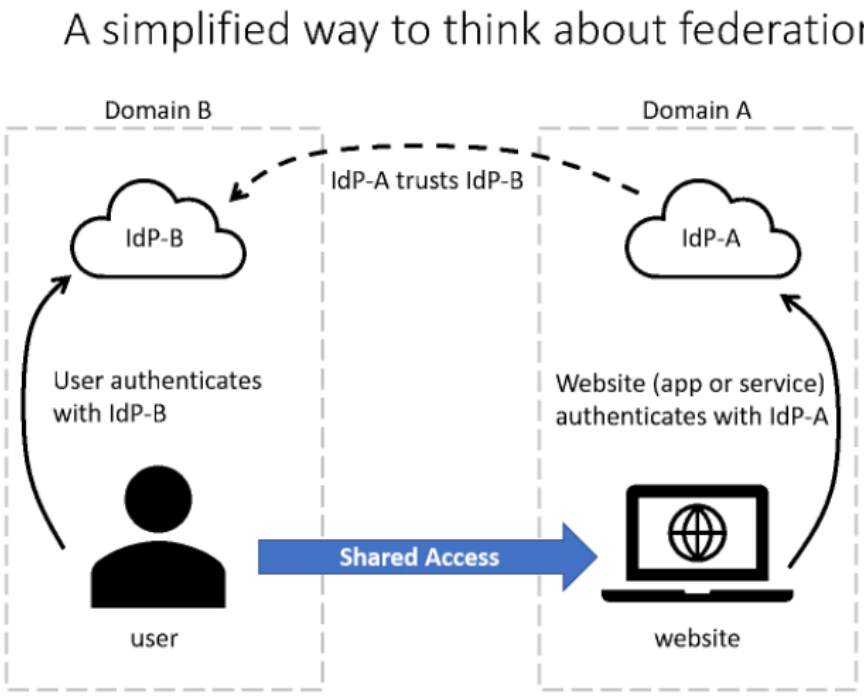
How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe the concept of federation

2 minutes

Federation enables the access of services across organizational or domain boundaries by establishing trust relationships between the respective domain's identity provider. With federation, there's no need for a user to maintain a different username and password when accessing resources in other domains.



*Although the function of the identity providers is depicted in a cloud, they do not need to be cloud based. The function of the identity providers can be on-premises.

The simplified way to think about this federation scenario is as follows:

- **The website, in domain A, uses the authentication services of Identity Provider A (IdP-A).**
- **The user, in domain B, authenticates with Identity Provider B (IdP-B).**
- **IdP-A has a trust relationship configured with IdP-B.**
- **When the user, who wants to access the website, provides his/her credentials to the website, the website trusts the user and allows access. This access is allowed because of the trust that is already established between the two identity providers.**

With federation, trust isn't always bidirectional. Although IdP-A may trust IdP-B and allow the user in domain B to access the website in domain A, the opposite isn't true, unless that trust relationship is configured.

A common example of federation in practice is when a user logs in to a third-party site with their social media account, such as Twitter. In this scenario, Twitter is an identity provider, and the third-party site might be using a different identity provider, such as Azure AD. There's a trust relationship between Azure AD and Twitter.

Next unit: Knowledge check

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Summary and resources

1 minute

In this module, you learned about authentication and authorization. You've learned about identity as the new security perimeter and the role of Active Directory. You also looked at the concept of federation to access resources that belong to another organization.

Now you've completed this module, you'll be able to:

- **Understand the difference between authentication and authorization.**
- **Describe the concept of identity as a security perimeter.**
- **Describe identity-related services.**

Learn more

For more information on the topics covered in this module, see:

- Authentication vs authorization
- Identity providers for External Identities
- Microsoft Entra ID documentation
- Compare Active Directory to Microsoft Entra ID (previously Azure Active Directory)

Module complete:

Review your Learning Path history

Explore other paths

How are we doing? ☆ ☆ ☆ ☆ ☆